

ON THE NON-EXISTENCE OF CERTAIN CLASSES OF PERFECT p -ARY SEQUENCES AND PERFECT ALMOST p -ARY SEQUENCES

CHANG LV

ABSTRACT. We obtain new non-existence results of perfect p -ary sequences with period n (called type $[p, n]$). The first case is a class with type $[p \equiv 5 \pmod{8}, p^a q n']$. The second case contains five types $[p \equiv 3 \pmod{4}, p^a q^l n']$ for certain p, q and l . Moreover, we also have similar non-existence results for PAPSs.

1. INTRODUCTION

Let n be a positive integer, p a rational prime and ζ_p a primitive p -th root of unity (we can take ζ_p to be $\exp(\frac{2\pi i}{p})$).

Definition 1.1. A complex sequence $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}, \dots)$ with period n is called a p -ary sequence (resp. an almost p -ary sequence) if $a_j = \zeta_p^{b_j}$ where $b_j \in \mathbb{Z}$ for all $j \geq 0$ (resp. $a_0 = 0$ and $a_j = \zeta_p^{b_j}$ where $b_j \in \mathbb{Z}$ for all $1 \leq j \leq n-1$).

A complex sequence $\mathbf{a} = (a_0, a_1, \dots, a_{n-1}, \dots)$ with period n is called *perfect* if $C_{\mathbf{a}}(t) = 0$ for all $1 \leq t \leq n-1$, where

$$C_{\mathbf{a}}(t) = \sum_{k=0}^{n-1} a_k \bar{a}_{k+t}$$

is the *autocorrelation* with a bar meaning the complex conjugation.

For simplicity, we denote a perfect p -ary (resp. an perfect almost p -ary) sequence with period n as a *PPS* (resp. *PAPS*) with *type* $[p, n]$.

A natural question is when PPSs (PAPSs) do exist. This is equivalent to the existence of certain kinds of relative difference sets. See [2, 9, 12] for details. Their results imply that PPSs (PAPSs) can be constructed if the corresponding relative difference sets exist. By using various techniques in combinatorial design theory, several classes of such sequences have been constructed (see [2, 9, 12, 10]). On the other hand, there are some nonexistence results on such sequences (and related difference sets), see [2, 9, 14, 17]. Here we need the concept of “self-conjugate”. See [21, 12].

Definition 1.2. Let p be a prime integer, $m = p^a m'$ where $a \geq 0$ and $(p, m') = 1$. We call p to be *self-conjugated* with respect to m if there exists $s \in \mathbb{Z}$ such that $p^s \equiv 1 \pmod{m'}$. Namely, if $-1 \in \langle p \rangle \subseteq (\mathbb{Z}/m'\mathbb{Z})^\times$.

Now we give a list of typical non-existence results of PPSs (PAPSs) with reference at the beginning of each item:

Date: December 20, 2016.

2000 Mathematics Subject Classification. 11R04, 94A15, 13C20, 11R45.

Key words and phrases. perfect sequences, p -ary and almost p -ary sequences, cyclotomic fields, class groups, Stickelberger relations, density theorem, CM-fields.

- (1) (Ma and Ng [14]) PPSs with type $[p, q^l n']$ where $p \neq q$ are two primes, $p \geq 3$, $(q, n') = 1$, q is self-conjugate w.r.t. p and $l \geq 1$ is odd.
- (2) (Liu and Feng [12]) PPSs with type $[p, p^a q^l n']$ where $p \equiv 3 \pmod{4}$ is a prime, q is another prime with $(q-1, p) = 1$, $\left(\frac{q}{p}\right) = 1$ and $\text{ord}_p(q)$ being odd, n' satisfies that $n' = 1$ or $\left(\frac{p'}{p}\right) = -1$ for all prime divisor p' of n' , $a \geq 1$ and l is odd such that $l < \lambda/s$ where $s = (p-1)/\text{ord}_p(q)$ and λ is the smallest odd integer such that $x^2 + py^2 = 4q^\lambda$ has solution (x, y) , $x, y \in \mathbb{Z}$.
- (3) (Liu and Feng [12]) PAPSs with type $[p, q^l n' + 1]$ where $p \equiv 3 \pmod{4}$, $p \mid q^l n' - 1$ is a prime, q, n', a and l are the same as the above (2).

In this article we have two main results. The first one shows the non-existence of PPSs with type $[p, p^a q n']$, where $p \equiv 5 \pmod{8}$ is a prime, q runs through a infinite set of primes and n' is the same as (2) in the above list.

Theorem 1.3. *Let $p \equiv 5 \pmod{8}$ be a prime and $\tilde{Q}_p = \{q \text{ is a prime} \mid \text{ord}_p(q) = (p-1)/4\}$. Then there exists a lower bound p_0 , and an infinite set $Q_p \subseteq \tilde{Q}_p$ for each p , such that if $p > p_0$, there is no PPSs with type $[p, n = p^a q n']$ for all integers $a \geq 1$, $q \in Q_p$ and n' such that $n' = 1$ or $\left(\frac{p'}{p}\right) = -1$ for all prime divisor p' of n' .*

Remark 1.4. Since $p \equiv 5 \pmod{8}$, we have $\text{ord}_p(q) = (p-1)/4$ is odd for all $q \in Q_p$. It follows that q is not self-conjugate w.r.t p , which says that our case is not contained in [14] ((1) in the above list). Moreover, our case is also different from [12] ((2) in the above list) since $p \not\equiv 3 \pmod{4}$. Thus our result is new.

In the second main result we obtain the non-existence of PPSs with five types:

Theorem 1.5. *Let $p \equiv 3$ be a prime, $q \neq p$ another prime and $f = \text{ord}_p(q)$. Suppose that the triple (p, f, l_0) equals to one of the following value:*

$$(31, 5, 1), (127, 9, 1), (127, 21, 3), (139, 23, 1), (151, 15, 3).$$

Define

$$\begin{aligned} \Xi_{31}(x) &= x^3 + x - 1, \\ \Xi_{127}(x) &= x^5 - x^4 - 2x^3 + x^2 + 3x - 1, \\ \Xi_{139}(x) &= x^3 - x^2 + x + 2, \\ \text{and } \Xi_{151}(x) &= x^7 - x^6 + x^5 + 3x^3 - x^2 + 3x + 1. \end{aligned}$$

Suppose further that for each $p \in \{31, 127, 139, 151\}$, the corresponding q satisfies that $\Xi_p(x) \equiv 0 \pmod{q}$ is not solvable. Then there is no PPPs with type $[p, n = p^a q^l n']$ for all integers $a \geq 1$, l odd, $1 \leq l \leq l_0$ and n' such that $n' = 1$ or $\left(\frac{p'}{p}\right) = -1$ for all prime divisor p' of n' .

Remark 1.6. For the same reason, this case is also not contained in [14] ((1) in the above list), and the result [12] ((2) in the above list) can only deal with type $[p, p^a q^l n']$ where $l < \lambda/s$. By direct calculation for (p, f) in the cases listed in Theorem 1.5, the corresponding $\lambda/s \leq l_0$. Thus the results in Theorem 1.5 are also new.

For the proofs of the two theorems, we need some facts in algebraic number theory which are contained in Section 2. With these preparations, we can prove Theorem 1.3 and 1.5 in Section 3 and 4, respectively.

We also have corresponding non-existence results for PAPSs, which are similar to Theorem 1.3 and 1.5. See the last section.

2. BASIC FACTS IN ALGEBRAIC NUMBER THEORY

The methods for proving non-existence results of PPSSs often involve algebraic number theory, mainly the basic arithmetic (ideals, units, class groups etc.) of cyclotomic fields and their subfields. The standard reference are [8] and [21]. In this section, we list some facts needed later, with proofs or references. The reader who does not care the proofs may skip to the next section.

For any number field F , denote by \mathfrak{o}_F the ring of integers of F . The latter ring is a Dedekind domain and we often consider the *fractional ideals* in it, which are \mathfrak{o}_F modules of the form \mathfrak{a}/α , where $\mathfrak{a} \subseteq \mathfrak{o}_F$ is an integral ideal and $\alpha \in \mathfrak{o}_F$ is a nonzero element. Denote by I_F the set of nonzero fractional ideals of F , which, one can show, under multiplication, is a free abelian group generated by all prime ideals. By a principal fractional ideal we mean a fractional ideal of the form $\alpha\mathfrak{o}_F$ where $\alpha \in F^\times$. Clearly, $P_F \subseteq I_F$ as a subgroup, and the quotient I_F/P_F , denoted by $Cl(F)$, is called the *class group* of F . Class groups play an important role in classical algebraic number theory. One of the nontrivial facts is that $Cl(F)$ is a finite abelian group for all F , and by $h(F)$ we denote the cardinality of $Cl(F)$, called the *class number* of F .

We need the basic knowledge of the decompositions of prime ideals in extension fields, the decomposition groups and the decomposition fields. We refer the reader to [8, Section I.6, Section III.7]. We also use properties of Artin maps and we need a corollary of class field theory, that is, there exists a finite unramified abelian extension H_F/F (called the *Hilbert class field*) for every F , such that the map $Cl(F) \rightarrow \text{Gal}(H_F/F)$ induced by Artin map is an isomorphism (see [8, Section V.13]). In particular, a prime ideal \mathfrak{p} of F is principal if and only if \mathfrak{p} splits completely in H_F , and we have $h(F) = [H_F : F]$.

For two subfields of the cyclotomic field $\mathbb{Q}(\zeta_{p^e})$ where p^e is a prime power, we have the divisibility of class numbers.

Lemma 2.1. *Let $L = \mathbb{Q}(\zeta_{p^e})$ and $F \subseteq E \subseteq L$ be two subfields of L . Then we have $h(F) \mid h(E)$.*

Proof. Since E/F is abelian and p is totally ramified in L/\mathbb{Q} , the result follows from [21, Proposition 4.11]. \square

Lemma 2.2. *Let E/F be two number fields. Then the canonical morphism $j_{E/F} : Cl(F) \rightarrow Cl(E)$ sending \mathfrak{a} to $\mathfrak{a}\mathfrak{o}_E$ is injective, provided that $\gcd(h(F), [E : F]) = 1$.*

Proof. The argument is quite simple. Let \mathfrak{a} be a fractional ideal of F such that $\mathfrak{a}\mathfrak{o}_E$ is trivial in $Cl(E)$. Then $\mathfrak{a}\mathfrak{o}_E = \alpha\mathfrak{o}_E$ for some $\alpha \in E$. Taking norm to F gives $\mathfrak{a}^{[E:F]} = N_{E/F}(\alpha)\mathfrak{o}_F$. But $\gcd(h(F), [E : F]) = 1$, therefore raising to the power to $[E : F]$ is an automorphism on $Cl(F)$. Hence \mathfrak{a} is also trivial in $Cl(F)$. This prove the injectivity. \square

For some cases, we have the following more strong statements.

Proposition 2.3. *Let $p \equiv 3 \pmod{4}$, $p > 3$ be a prime and $L = \mathbb{Q}(\zeta_{p^e})$, $F := \mathbb{Q}(\sqrt{-p})$. It is well-known that F is a subfield of L . Let E be any number field such that $F \subseteq E \subseteq L$. Then $j_{E/F} : Cl(F) \rightarrow Cl(E)$ is injective.*

Proof. The statement of [19, Corollary to Proposition 4, pp. 2723] says that if M is any subfield of $\mathbb{Q}(\zeta_n)$ with the only roots of unity ± 1 , and \mathfrak{a} is an ideal of M such that $\mathfrak{a}\bar{\mathfrak{a}}$ is principal in M and \mathfrak{a} is principal in $\mathbb{Q}(\zeta_n)$, then \mathfrak{a}^4 is principal in M . Now we apply this result with $M = F$ and $n = p$. Let \mathfrak{a} be any ideal of F that is principal in E . Then \mathfrak{a} become principal in L . Also $\mathfrak{a}\bar{\mathfrak{a}}$ is clearly principal in F since F is imaginary quadratic. It follows that \mathfrak{a}^4 is principal in F . On the other hand, by Gauss' genus theory (c.f. [21, Theorem 10.4 (b)]) or Lemma 2.8 below, we know that $h(F)$ is odd. Thus \mathfrak{a} is principal in F . The injectivity follows. \square

To show that the set Q_p in Theorem 1.3 is infinite in the subsequent section, we need a special case of Chebotarev's density theorem and compare class numbers. We first introduce

Definition 2.4. Let K be any number field and S be a set of prime ideals of \mathfrak{o}_K . Denote all prime ideals of \mathfrak{o}_K by \mathcal{P}_K . The *Dirichlet density* of S is the limit (if exists)

$$\delta = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})^s}}{\sum_{\mathfrak{p} \in \mathcal{P}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathfrak{p})^s}},$$

denoted as $\delta(S) = \delta$.

There may exists some other definitions but they are equivalent. Now we have the statement:

Proposition 2.5. *Let L/K be abelian extension of two number fields with Galois group G and fix an element $\sigma \in G$. Let S be the set of prime ideal \mathfrak{p} of K whose Artin map $(\mathfrak{p}, L/K)$ is σ . Then S has Dirichlet density $\delta(S) = 1/\#G$.*

Proof. See, for example [16, Theorem 13.4]. □

Next we consider a wider class of number fields containing cyclotomic fields, namely:

Definition 2.6. A *CM-field* E is a totally imaginary quadratic extension of a totally real number field E^+ . The field E^+ is the *maximal real subfield* of E . That a field is totally real (resp. imaginary) means that all embeddings of the field into \mathbb{C} is real (resp. imaginary).

As mentioned above, we want to compare certain class numbers. For this purpose, we mainly use the following facts about CM-fields:

Proposition 2.7 (c.f. [21], Section 4, pp. 38-43). Let E be CM and E^+ its maximal real subfield. For convenience, let h, U, W, R and d be the class number, unit group, group of roots of unity, regulator and discriminant of E respectively, and let h^+, U^+, R^+ and d^+ denote the corresponding objects for E^+ . Then we have:

- (a) The class number h^+ divides h , and the quotient h^- is called the *relative class number*.
- (b) The index $Q := [U : WE^+] = 1$ or 2 .
- (c) The quotient $R/R^+ = \frac{1}{Q}2^r$, where $r := \frac{1}{2}[E : \mathbb{Q}] - 1$.
- (d) (Brauer-Siegel theorem) Suppose E runs through a sequence of number fields normal over \mathbb{Q} (not necessary CM) such that

$$\frac{[E : \mathbb{Q}]}{\log |d_E|} \rightarrow 0.$$

Then

$$\frac{\log(h(E)R_E)}{\log \sqrt{|d_E|}} \rightarrow 1.$$

We also need a result for the parity of the class numbers of a special class of CM-fields.

Lemma 2.8 (See [5], Corollary 13.13). Let E be CM which is Galois over \mathbb{Q} with $\text{Gal}(E/\mathbb{Q})$ a cyclic group of order 2^k , $k \geq 1$. Then $h(E)$ is odd if and only if exactly one finite rational prime ramifies in E/\mathbb{Q} .

Next we introduce Stickelberger ideals. Suppose p is a prime, $K = \mathbb{Q}(\zeta_p)$ and $G = \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

Definition 2.9. The *Stickelberger element* $\theta = \theta_p \in \mathbb{Q}[G]$ is defined by

$$\theta = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left\{ \frac{a}{p} \right\} \sigma_a^{-1}$$

where $\left\{ \frac{a}{p} \right\} = \frac{a}{p} - \left[\frac{a}{p} \right]$, and the *Stickelberger ideal* S_p of $\mathbb{Z}[G]$ is defined by

$$S_p = \mathbb{Z}[G]\theta \cap \mathbb{Z}[G].$$

We mainly use these following properties of the Stickelberger ideal:

Proposition 2.10. *We have:*

- (a) For $(c, p) = 1$, the element $(c - \sigma_c)\theta$ are in S_p .
- (b) The Stickelberger ideal S_p annihilates the ideal class group $Cl(M)$, where M is a subfield of K such that p is the minimal integer with the property that $M \subseteq \mathbb{Q}(\zeta_p)$.

Proof. See [21, Lemma 6.9 and Theorem 6.10]. □

Notation. Through this paper, we fix the following notation. Let p be an odd prime and denote ζ_k a primitive k -th root of unity. Let $K = \mathbb{Q}(\zeta_p)$. In the remaining of this paper we mainly deal with $\mathbb{Q}(\zeta_p)$ and write $\zeta = \zeta_p$ for simplicity. Let $G = \text{Gal}(K/\mathbb{Q})$. It's well-known that $G \cong (\mathbb{Z}/N\mathbb{Z})^\times$, the isomorphism being $c \mapsto (\sigma_c : \zeta \mapsto \zeta^c)$ for $c \in (\mathbb{Z}/N\mathbb{Z})^\times$.

The starting point of our method is the following

Proposition 2.11. *If there exist PPS with type $[p, n]$, then $p \mid n$ and $\alpha\bar{\alpha} = n$ for some $\alpha \in \mathbb{Z}[\zeta_p]$.*

Proof. The result is obtained by applying different sets. See, for example, [12, Theorem 1.4 (1)] and the remarks after it. □

Thus for our purpose we need to investigate the equation $\alpha\bar{\alpha} = n$ where $\alpha \in \mathbb{Z}[\zeta_p]$. So we mainly study the idealic behaviour of each p dividing n , in the cyclotomic field K .

3. NON-EXISTENCE RESULT FOR PPSS WITH TYPE $[p \equiv 5 \pmod{8}, p^a q n']$

In this section, we will prove Theorem 1.3. We start with the definition of Q_p . As the assumptions in the theorem, let $p \equiv 5 \pmod{8}$ be a prime and

$$\tilde{Q}_p = \{ q \text{ is a prime} \mid \text{ord}_p(q) = (p-1)/4 \}.$$

Let $q \in \tilde{Q}_p$ so $\text{ord}_p(q) = (p-1)/4$. Let $K = \mathbb{Q}(\zeta_p)$ and E be the unique subfield of K having degree 4 over \mathbb{Q} . Then the order of q modulo p tells us that E is the decomposition group of q in K and depends only in p . Thus we write $E_p = E$ and it is well known that K contains the unique real quadratic subfield $F_p = \mathbb{Q}(\sqrt{p}) \subset E_p$.

Actually one can define

$$(3.1) \quad Q_p = \left\{ q \in \tilde{Q}_p \mid \begin{array}{l} \text{there is a prime ideal } \mathfrak{Q} \text{ in } E_p \text{ lying over } q \text{ such that} \\ \mathfrak{Q} \text{ is not principal while } \mathfrak{q} = \mathfrak{P} \cap \mathfrak{o}_{F_p} \text{ is principal} \end{array} \right\}.$$

To show that Q_p is infinite, we only need to show that the Dirichlet density $\delta(Q_p) > 0$, since any finite set has zero density by the definition.

Lemma 3.2. *Let L/M be cyclic extension of two number fields such that they are both Galois over \mathbb{Q} and there is some finite prime in M totally ramified in L . Define*

$$S(f, L/M) = \left\{ p \text{ is a prime number} \left| \begin{array}{l} p \text{ split completely in } M \text{ and there is a principal} \\ \text{prime ideal } \mathfrak{p} \text{ in } M \text{ lying over } p \text{ and the order} \\ \text{of the Artin map } (\mathfrak{p}, L/M) \text{ is } f \end{array} \right. \right\}.$$

Then we have

$$\delta(S(f, L/M)) = \frac{\varphi(f)}{[L : \mathbb{Q}] h(M)},$$

with φ being the Euler's totient function.

Proof. Let H_M be the Hilbert class field of M . Since there is a finite prime totally ramified in L/M and H_M/M is unramified, we have $H_M \cap L = M$. Hence we have a natural isomorphism

$$(3.3) \quad \text{Gal}(LH_M/M) \cong \text{Gal}(L/M) \times \text{Gal}(H_M/M)$$

and that LH_M/M is an abelian extension of degree $[L : M] h(M)$. Let S denote the set of prime ideal \mathfrak{p} in M such that \mathfrak{p} is principal and $(\mathfrak{p}, L/M)$ has order f . Fix an element $\sigma \in \text{Gal}(L/M)$ having order f . Since L/M is cyclic, we know that σ^k , $k \in (\mathbb{Z}/f\mathbb{Z})^\times$ are exactly all the element in $\text{Gal}(L/M)$ having order f . Moreover, we can interpret the constraint that \mathfrak{p} is principal as $(\mathfrak{p}, H_M/M) = 1$. Under the isomorphism (3.3), we know that

$$S = \{ \mathfrak{p} \text{ in } M \mid (\mathfrak{p}, LH_M/M) = (\sigma^k, 1) \in \text{Gal}(L/M) \times \text{Gal}(H_M/M), k \in (\mathbb{Z}/f\mathbb{Z})^\times \}.$$

A direct application of Proposition 2.5 yields

$$\delta(S) = \frac{\varphi(f)}{[L : M] h(M)}.$$

Let S_1 be the set of primes of M having relative degree one over \mathbb{Q} . An elementary argument (c.f. [8, Section 4.6, (4.6.2)] tells us that $\delta(S \cap S_1) = \delta(S)$. Let $\mathfrak{p} \in S \cap S_1$ and $p = \mathfrak{p} \cap \mathbb{Z}$. Since M/\mathbb{Q} is Galois, p splits completely in M and every \mathfrak{p}' in M lying over p is also principal. Moreover, the assumption that L/\mathbb{Q} is Galois ensures that all $(\mathfrak{p}', L/M)$ are conjugate and hence having the same order f . It follows that

$$\delta(S(f, L/M)) = \frac{1}{[M : \mathbb{Q}]} \delta(S \cap S_1) = \frac{\varphi(f)}{[L : \mathbb{Q}] h(M)}.$$

The proof is complete. □

The following lemma gives a lower bound for the density of Q_p .

Lemma 3.4. *Let $p \equiv 5 \pmod{8}$ be a prime and Q_p defined by (3.1). Then we have*

$$\delta(Q_p) \geq \frac{\varphi((p-1)/4)}{p-1} \left(\frac{1}{h(F_p)} - \frac{1}{h(E_p)} \right),$$

Proof. Clearly K and E_p are both Galois over \mathbb{Q} . Let $q \in Q_p$ and \mathfrak{Q} be any prime in E_p lying over q . Since E_p is the decomposition field of q in K , q splits completely in E_p . Thus we have $(\mathfrak{Q}, K/F_p) = (q, K/\mathbb{Q})$, which has order $(p-1)/4$. Applying Lemma 3.2 we obtain

$$\delta(S(\frac{p-1}{4}, K/E_p)) = \frac{\varphi((p-1)/4)}{(p-1)h(E_p)}.$$

A similar analyze for K/F_p yields

$$\delta(S(\frac{p-1}{4}, K/F_p)) = \frac{\varphi((p-1)/4)}{(p-1)h(F_p)}.$$

In view of $Q_p = S(\frac{p-1}{4}, K/F_p) \setminus S(\frac{p-1}{4}, K/E_p)$, we have

$$\begin{aligned} \delta(Q_p) &= \delta(S(\frac{p-1}{4}, K/F_p) \setminus S(\frac{p-1}{4}, K/E_p)) \\ &\geq \delta(S(\frac{p-1}{4}, K/F_p)) - \delta(S(\frac{p-1}{4}, K/E_p)) \\ &= \frac{\varphi((p-1)/4)}{p-1} \left(\frac{1}{h(F_p)} - \frac{1}{h(E_p)} \right), \end{aligned}$$

where the second line is due to the fact that we can sum the densities of two disjoint sets, which is easily seen by the definition. So we finish the proof. \square

Our next goal is to show that if $p > p_0$ for some p_0 , the density $\delta(Q_p)$ is positive. Recall that $E_p \subseteq K = \mathbb{Q}(\zeta_p)$ contains $F_p = \mathbb{Q}(\sqrt{p})$. Since $\text{ord}_p(q) = (p-1)/4$ is odd, the complex conjugation does not fix E_p . It follows that E_p is a totally imaginary cyclic extension of \mathbb{Q} , and hence a CM-field with $E_p^+ = F_p$ being the maximal real subfield. We write h_p for $h(E_p)$, and h_p^+ for $h(E_p^+) = h(F_p)$. Thus from Proposition 2.7 (a) we know that $h_p = h_p^+ h_p^-$ for a positive integer h_p^- , which is the relative class number for E_p . We now consider the asymptotic behaviour of h_p^- .

Lemma 3.5. *With the previous notation we have*

$$\log h_p^- \geq \frac{1}{2}(\log p)(1 + o(1)) \quad \text{as } p \rightarrow \infty.$$

Proof. We follow the same method in [21, Section 4]. But the case here is simpler. Let U_p, W_p, R_p and d_p be the unit group, group of roots of unity, regulator and discriminant of E_p respectively, and let U_p^+, R_p^+ and d_p^+ denote the corresponding objects for E_p^+ . The ideal is to use Brauer-Siegel theorem (Proposition 2.7 (d)) for E_p/E_p^+ . To verify the assumption of the theorem, we need to estimate the discriminants of E_p^+ and E_p . Recall that $E_p^+ = F_p = \mathbb{Q}(\sqrt{p})$ and clearly we know that $d_p^+ = p$. Then the relative discriminant formula (c.f. [11, pp. 82]) gives

$$|d_p| = N_{E_p/\mathbb{Q}}(\mathcal{D}(E_p/E_p^+)) |d_p^+|^{[E_p:E_p^+]},$$

where $\mathcal{D}(E_p/E_p^+)$ is the relative different, which is a integral ideal in \mathfrak{o}_{E_p} . Thus we have

$$(3.6) \quad |d_p| \geq |d_p^+|^{[E_p:E_p^+]} = p^2.$$

Since the we have $[E_p : \mathbb{Q}] = 2[E_p^+ : \mathbb{Q}] = 4$ for all p , we know that

$$\frac{[E_p : \mathbb{Q}]}{\log |d_p|} \rightarrow 0 \quad \text{and} \quad \frac{[E_p^+ : \mathbb{Q}]}{\log |d_p^+|} \rightarrow 0$$

and Brauer-Siegel theorem applies. It follows that

$$\begin{aligned} \log(h_p R_p) &= \frac{1}{2} \log d_p + o(\log d_p) \\ \text{and } \log(h_p^+ R_p^+) &= \frac{1}{2} \log d_p^+ + o(\log d_p^+) \end{aligned}$$

By Proposition 2.7 (b) and (c) we have

$$\log \left(\frac{R_p}{R_p^+} \right) = O(1).$$

Hence, noting that $\log d_p^+ \leq \frac{1}{2} \log d_p$ by (3.6), we have

$$\begin{aligned} \log h_p^- &= \log(h_p R_p) - \log(h_p^+ R_p^+) - \log \left(\frac{R_p}{R_p^+} \right) \\ &= \frac{1}{2} \log d_p - \frac{1}{2} \log d_p^+ + o(\log d_p) + O(1) \\ &\geq \frac{1}{2} \log d_p - \frac{1}{4} \log d_p + o(\log d_p) \\ &= \frac{1}{4} (\log d_p) (1 + o(1)) \\ &\geq \frac{1}{2} (\log p) (1 + o(1)). \end{aligned}$$

□

Proposition 3.7. *Let notation be as before, $p \equiv 5 \pmod{8}$ a prime and Q_p defined by (3.1). Then we have*

(a) *the equation*

$$(3.8) \quad \beta \bar{\beta} = q, \quad \beta \in \mathfrak{o}_{E_p}$$

has no solution for all $q \in Q_p$;

(b) *if $h_p > h_p^+$ then the set Q_p is infinite;*

(c) *there exists a lower bound p_0 such that if $p > p_0$, then the set Q_p is infinite.*

Proof. Let $p \equiv 5 \pmod{8}$ and $q \in Q_p$. Recall that $\text{ord}_p(q) = (p-1)/4$ is odd and E_p is the decomposition field of q in $K = \mathbb{Q}(\zeta_p)$ with $[E_p : \mathbb{Q}] = 4$, so we have the prime decomposition

$$q\mathfrak{o}_{E_p} = \mathfrak{Q}_1 \mathfrak{Q}_2 \mathfrak{Q}_3 \mathfrak{Q}_4.$$

It is also noted before that the complex conjugation is not in the decomposition group of q . Thus we may assume $\mathfrak{Q}_3 = \bar{\mathfrak{Q}}_1$ and $\mathfrak{Q}_4 = \bar{\mathfrak{Q}}_2$.

Now we assume that the equation (3.8) has solution $\beta \in \mathfrak{o}_{E_p}$, so we have

$$\beta \bar{\beta} \mathfrak{o}_{E_p} = q\mathfrak{o}_{E_p} = \mathfrak{Q}_1 \mathfrak{Q}_2 \bar{\mathfrak{Q}}_1 \bar{\mathfrak{Q}}_2.$$

It follows that the only possible decompositions of β are

$$(3.9) \quad \beta \mathfrak{o}_{E_p} = \mathfrak{Q}_1 \mathfrak{Q}_2, \mathfrak{Q}_1 \bar{\mathfrak{Q}}_2, \bar{\mathfrak{Q}}_1 \mathfrak{Q}_2 \text{ or } \bar{\mathfrak{Q}}_1 \bar{\mathfrak{Q}}_2.$$

Write $\text{Gal}(E_p/\mathbb{Q}) = \langle \sigma \rangle$ with σ of order 4. It follows that we can assume

$$\mathfrak{Q}_1^{\sigma^t} = \mathfrak{Q}_{t+1}, \quad t = 0, 1, \dots, 3.$$

Then (3.9) tells us that

$$1 = \mathfrak{Q}_1^{1+\sigma}, \mathfrak{Q}_1^{1+\sigma^3}, \mathfrak{Q}_1^{\sigma^2+\sigma} \text{ or } \mathfrak{Q}_1^{\sigma^2+\sigma^3} \text{ in } Cl(E_p).$$

Correspondingly, rising to the power to $1-\sigma$, $1-\sigma^3$, $\sigma^2-\sigma$ or $\sigma^2-\sigma^3$, we obtain the same equation

$$(3.10) \quad \mathfrak{Q}_1^{1-\sigma^2} = 1 \text{ in } Cl(E_p).$$

On the other hand, by the definition (3.1), we know that there is a prime ideal \mathfrak{Q} in E_p over q such that \mathfrak{Q} is not principal while $\mathfrak{q} = \mathfrak{P} \cap \mathfrak{o}_{F_p}$ is principal. With loss of generality, we may assume that $\mathfrak{Q}_1 = \mathfrak{Q}$. Since \mathfrak{q} is principal, so is $\mathfrak{q}\mathfrak{o}_{E_p} = \mathfrak{Q}_1\bar{\mathfrak{Q}}_1$, which means that

$$\mathfrak{Q}_1^{1+\sigma^2} = 1 \text{ in } Cl(E_p).$$

Combining with (3.10), we have $\mathfrak{Q}_1^2 = 1$ in $Cl(E_p)$. However, since p is the unique finite rational prime that ramifies in E_p/\mathbb{Q} , Lemma 2.8 tells us that $h(E_p)$ is odd. It follows that $\mathfrak{Q}_1 = 1$ in $Cl(E_p)$, which is a contradiction because Q_1 is not principal by the previous argument. Thus the assumption we made before is false and we complete the proof for (a).

Next, let $p \equiv 5 \pmod{8}$ and suppose that $h_p > h_p^+$. By Lemma 3.4, we know that

$$\delta(Q_p) \geq \frac{\varphi((p-1)/4)}{p-1} \left(\frac{1}{h_p^+} - \frac{1}{h_p} \right) > 0.$$

Thus Q_p is a infinite set and (b) is correct.

For the last assertion (c), recall that E_p/F_p is CM and we use Lemma 3.5 to obtain

$$h_p^- \rightarrow \infty \quad \text{as } p \rightarrow \infty.$$

It follows that there exists a lower bound p_0 such that if $p > p_0$, then $h_p^- > 1$, i.e. $h_p > h_p^+$. It follow by (b) that Q_p is infinite for all $p > p_0$. That's all the proof. \square

Although we have shown that Q_p is infinite, one do not know whether a given q is in Q_p . However, this can be done when we know the Hilbert class field H_{F_p} and H_{E_p} of F_p and E_p , respectively. We now describe this method as follows.

Suppose in general, L is a number field. Let $\Xi_L(x) \in \mathfrak{o}_L[x]$ be an irreducible polynomial having a root that generates the Hilbert class field H_L over L , and we call Ξ_L the *Hilbert class polynomial*. If there is a subfield M such that L/M is cyclic with $h(M) = 1$, then there exist an auxiliary field $K = K_{L/M}$ such that $H_L = KM$ and $M = K \cap L$. See [6, Proposition 3]. It follows that we can choose $\Xi_L(x)$ with coefficients in \mathfrak{o}_M .

Lemma 3.11. *Let L/M , $\Xi_L(x) \in \mathfrak{o}_M[x]$ be as before, and \mathfrak{P} a prime ideal of L having relative degree one over M not dividing the discriminant of Ξ_L . Let $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_M$. Then \mathfrak{P} is principal if and only if $\Xi_L(x) = 0$ has a solution over $\mathfrak{o}_M/\mathfrak{p}$.*

Proof. Since H_L is the Hilbert class field of L , so we know that \mathfrak{P} is principal if and only if \mathfrak{P} splits completely in H_L . Note that \mathfrak{P} does not divide the discriminant of Ξ_L . Then a direct application of Kummer theorem (c.f. [11, Proposition 25, Chapter I.8]) tells us that \mathfrak{P} splits completely in H_L if and only if $\Xi_L(x) = 0$ has a solution over $\mathfrak{o}_L/\mathfrak{P}$, which is to say that $\Xi_L(x) = 0$ has a solution over $\mathfrak{o}_E/\mathfrak{p}$, since \mathfrak{P} is a prime ideal of L having relative degree one over M . \square

In our case where E_p/\mathbb{Q} is cyclic and F_p is real quadratic, we know that both $K_{E_p/\mathbb{Q}}$ and $K_{F_p/\mathbb{Q}}$ exist. Hence we have Ξ_{E_p} and Ξ_{F_p} with integral coefficients. Then we have

Corollary 3.12. *Fix a prime $p \equiv 5 \pmod{8}$ and let the irreducible polynomials $\Xi_{E_p}(x)$ and $\Xi_{F_p}(x)$ in $\mathbb{Z}[x]$ be as before. Given $q \in \tilde{Q}_p$ not dividing the discriminants of the two polynomials, then we have $q \in Q_p$ if and only if $\Xi_{F_p}(x) \equiv 0 \pmod{q}$ is solvable while $\Xi_{E_p}(x) \equiv 0 \pmod{q}$ is not.*

Proof. Apply Lemma 3.11 to E_p/\mathbb{Q} and F_p/\mathbb{Q} and then the result follows from the definition of Q_p . \square

Now the problem left is to find the Hilbert class polynomials for E_p and F_p . For the real quadratic field F_p , the polynomial Ξ_{F_p} is quite easy to obtain (c.f. Stark's method described by Cohen [4], who also gives a list of these polynomials). As for E_p , which is a CM-field and is cyclic of degree 4 over \mathbb{Q} , we could use complex multiplication to calculate Ξ_{E_p} . This is more complicated than the imaginary quadratic case where elliptic curves and the j -invariant are enough. In the case of degree 4 CM-fields, we work with curves of genus 2, three j -invariants and three igusa class polynomials. See Streng [20] or Enge et al. [7] for complete description of the method. There is also an implementation of the algorithm by Enge et al., CMH [1], which enables us to calculate the individual igusa class polynomials. We can use igusa class polynomials instead of the Hilbert class polynomial, or calculate the Hilbert class polynomial by them. This solves the whole problem. We give an example to illustrate this method.

Example 3.13. *Let $p = 101$, and*

$$\begin{aligned} \Xi(x) = & x^5 - 1237224274356339549352800 x^4 + 57176933499148 \\ & 833882237435031573248869838360576 x^3 \\ & + 2514056979190981026432576749022147825857609219676093 \\ & 86630877092098080768 x^2 \\ & - 1023671146645480759972364788108250129958692705554245 \\ & 7706457967352624977868378319649505280 x \\ & + 1530499568113365603805244886351320629567046080073893 \\ & 31920814045884605474516662499805087162052695075848192. \end{aligned}$$

If $q \in \tilde{Q}_p$ and $q \neq 2542000616863$, then $q \in Q_p$ if and only if $\Xi(x) \equiv 0 \pmod{q}$ is solvable.

Proof (sketch). For $p = 101$ we have $F_p = \mathbb{Q}(\sqrt{101})$ and $E_p = \mathbb{Q}(\alpha)$ where α is a root of $x^4 + 101x^2 + 101$. Using GP calculator (see [18]) we obtain that $h_p^+ = h(F_p) = 1$ and $h(E_p) = 5$. Using CMH (see above), we obtain that the first igusa class polynomial of E_p is $\Xi(x)$, which is also the Hilbert class polynomial of E_p since it already has degree 5. Also we know $q = 2542000616863$ is the only prime in \tilde{Q}_p that divides the discriminant of $\Xi(x)$. The assertion follows by Corollary 3.12. \square

Let us turn to the

Proof of Theorem 1.3. If there exist PPS with type $[p, n]$, where $p \equiv 5 \pmod{8}$ be a prime and $n = p^a q n'$, then by Proposition 2.11 we know that

$$\alpha \bar{\alpha} = n = p^a q n' \text{ for some } \alpha \in \mathfrak{o}_K = \mathbb{Z}[\zeta_p].$$

Here $K = \mathbb{Q}(\zeta_p)$. [12, Lemma 2.4 (2)] tells us that

$$\alpha_1 \bar{\alpha}_1 = p^a q \text{ for some } \alpha_1 \in \mathfrak{o}_K.$$

Next by [12, Lemma 2.4 (1)] we obtain that

$$\alpha_2 \bar{\alpha}_2 = q \text{ for some } \alpha_2 \in \mathfrak{o}_K.$$

We may assume $p > 5$. Then $\text{ord}_p(q) = (p-1)/4 > 1$ and so $(p, q-1) = 1$. Recall that E_p is the decomposition field of q in K , so we use [12, Lemma 2.4 (3)] to obtain that

$$\beta \bar{\beta} = q \text{ for some } \beta \in \mathfrak{o}_K \text{ and } \beta^2 \in \mathfrak{o}_{E_p}.$$

But $[K : E_p] = \text{ord}_p(q) = (p-1)/4$ is odd, so in fact we have $\beta \in \mathfrak{o}_{E_p}$.

Thus the theorem follows from Proposition 3.7. \square

4. NON-EXISTENCE RESULT FOR PPSS WITH TYPE $[p \equiv 3 \pmod{4}, p^a q^l n']$ FOR CERTAIN p, q
AND l

We will prove Theorem 1.5 in this section. The main ideal is the application of Stickelberger relations, which was used by the first author and Jianing Li [13] for showing non-existence results for some bent functions. First we fix some additional notation. Suppose $n = p^a q^l n'$ and $p \equiv 3 \pmod{4}$ be as in the theorem. Then we know that $f := \text{ord}_p(q)$ is odd. Thus $g := \frac{\varphi(p)}{f}$ is even and we set $u = g/2$. Recall that $K = \mathbb{Q}(\zeta_p)$ and let E be the unique subfield of K having degree g over \mathbb{Q} . Then E is the decomposition group of q in K and is CM with $E^+ = E \cap \mathbb{R}$ its maximal real subfield (the argument is similar as before, see Section 3). It is well known that K contains the unique imaginary quadratic subfield $F = \mathbb{Q}(\sqrt{-p}) \subset E$.

Suppose the prime decomposition of q in E is

$$(4.1) \quad q\mathfrak{o}_E = \mathfrak{Q}_1 \mathfrak{Q}_2 \dots \mathfrak{Q}_g.$$

If there is a PPSS with type $[p, n]$, then as in the proof of Theorem 1.3, a similar argument using Proposition 2.11 and [12, Lemma 2.4] yields the equation

$$\beta \bar{\beta} = q^l, \quad \beta \in \mathfrak{o}_E.$$

Since f is odd, the complex conjugation is not in the decomposition group of q . Thus we may assume $\mathfrak{Q}_{u+k} = \bar{\mathfrak{Q}}_k$, $k = 1, 2, \dots, u$. Then we have

$$\beta \bar{\beta} \mathfrak{o}_E = \prod_{k=1}^u \mathfrak{Q}_k^{l_k} \bar{\mathfrak{Q}}_k^{l_k}.$$

So

$$(4.2) \quad \beta \mathfrak{o}_E = \prod_{k=1}^u \mathfrak{Q}_k^{l_k} \bar{\mathfrak{Q}}_k^{\bar{l}_k}$$

where l_k, \bar{l}_k are nonnegative integer such that $l_k + \bar{l}_k = l$ for all $k = 1, 2, \dots, u$.

For convenience we write x_k for \mathfrak{Q}_k in $Cl(E)$ and view $Cl(E)$ additively. Hence (4.2) becomes

$$(4.3) \quad \sum_{k=1}^u (l_k x_k + \bar{l}_k \bar{x}_k) = 0$$

where $l_k + \bar{l}_k = l$, $k = 1, 2, \dots, u$.

Thus we obtain the

Proposition 4.4. *With the above notation, if (4.3) has no nonnegative integral solution (l_1, l_2, \dots, l_g) , where $l_k + \bar{l}_k = l_0$ and $l_{u+k} := \bar{l}_k$, $k = 1, 2, \dots, u$, then there is no PPSS with type $[p, n]$.*

To show (4.3) is not solvable in the above sense, we have to exploit the relations between x_k 's in $Cl(E)$. By (4.1) we have

$$(4.5) \quad \sum_{k=1}^g x_k = 0.$$

We want to find more relations.

Let $K^+ = K \cap \mathbb{R} = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Then Miller's work on class number of K^+ gives

Theorem 4.6 ([15], Theorem 1.1). The class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is 1 if $p \leq 151$ is a prime.

From now on we suppose $p \leq 151$. Clearly, $E^+ \subseteq K^+$. Then by Miller's result and Lemma 2.1, we have $h(E^+) = h(K^+) = 1$. Now $q\mathfrak{o}_{E^+} = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_u$ where $\mathfrak{q}_k\mathfrak{o}_E = \mathfrak{Q}_k\bar{\mathfrak{Q}}_k$, and all \mathfrak{q}_k 's are principal since $h(E^+) = 1$. This implies the relations

$$(4.7) \quad x_k + x_{u+k} = 0, \quad k = 1, 2, \dots, u.$$

However, these relations above are not enough. We need the Stickelberger ideal introduced in Section 2. Let $\mathfrak{Q} = \mathfrak{Q}_1$ and correspondingly $x = x_1$. Let c be an integer not divisible by p . Since it is well-known that p is the minimal integer such that $F \subseteq \mathbb{Q}(\zeta_p)$, it follows that p is also the minimal one such that $E \subseteq \mathbb{Q}(\zeta_p)$. By Proposition 2.10, we have

$$(4.8) \quad (c - \sigma_c)\theta \mathfrak{Q} = 1 \text{ in } Cl(E).$$

Let w be a primitive root mod p . Recall $G = \text{Gal}(K/\mathbb{Q})$. Then the decomposition group of q in K is $\langle q \rangle = \langle w^g \rangle \subseteq G = (\mathbb{Z}/p\mathbb{Z})^\times$. It follows that we can assume

$$(4.9) \quad \sigma_w^{tg+s}(x) = x_{s+1}, \quad t \in \mathbb{Z}, \quad s = 0, 1, \dots, g-1.$$

Let $k_{c,a} = \left[\frac{ca}{p}\right]$ for any integer a . We have

$$\begin{aligned} (c - \sigma_c)\theta &= (c - \sigma_c) \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left\{ \frac{a}{p} \right\} \sigma_a^{-1} \\ &= \sum_a \left(c \left\{ \frac{a}{p} \right\} - \left\{ \frac{ca}{p} \right\} \right) \sigma_a^{-1} \\ &= \sum_{a=1}^{p-1} k_{c,a} \sigma_a^{-1} \quad (\text{the definition of } k_{c,a}) \\ &= \sum_{s=0}^{p-2} k_{c,w^{-s}} \sigma_w^s \quad (w^{-s} \text{ means } w^{-s} \pmod{p}) \\ &= \sum_{t=0}^{f-1} \sum_{s=0}^{g-1} k_{c,w^{-(tg+s)}} \sigma_w^{tg+s} \end{aligned}$$

Then by (4.8) we have

$$\begin{aligned} 1 &= \mathfrak{Q} \sum_{t=0}^{f-1} \sum_{s=0}^{g-1} k_{c,w^{-(tg+s)}} \sigma_w^{tg+s}, \\ \text{i.e., } 0 &= \sum_{t=0}^{f-1} \sum_{s=0}^{g-1} k_{c,w^{-(tg+s)}} \sigma_w^{tg+s}(x) \\ &= \sum_{t=0}^{f-1} \sum_{s=0}^{g-1} k_{c,w^{-(tg+s)}} x_{s+1} \quad (\text{by (4.9)}) \\ &= \sum_{s=1}^g m_{c,s} \sum_{t=0}^{f-1} k_{c,w^{-tg-s+1}} x_s. \end{aligned}$$

If we set

$$(4.10) \quad m_{c,s} = \sum_{t=0}^{f-1} k_{c,w^{-tg-s+1}}$$

we have $p-1$ linear equations

$$\sum_{s=1}^g m_{c,s} x_s = 0, \quad c = 1, 2, \dots, p-1.$$

We now combine these $p-1$ equations, together with the equation (4.5) and the u equations (4.7), to give a whole collection of equations

$$(4.11) \quad XM_{p,f}^T = 0$$

where $M_{p,f}$ is a $(p+u) \times g$ matrix with integer entries made of the coefficients of all the $p+u$ equations and $X = (x_1, x_2, \dots, x_g)$. Note that $M_{p,f}$ depends only on p and f . To simplify these relations of x_1, x_2, \dots, x_g , we need to calculate the *Hermite normal form* of $M_{p,f}$. By the well-known result (c.f. [3, Chapter 2.4.2]) for the existence of the Hermite normal form, there exists a unique matrix $U_{p,f} \in \text{GL}_{p+u}(\mathbb{Z})$, such that $H_{p,f} = M_{p,f}^T U_{p,f}$ is a Hermite normal form. It follows from (4.11) that

$$XH_{p,f} = 0.$$

In fact, $H_{p,f}$ can be obtained by applying a finite sequence of elementary row operations over \mathbb{Z} from $M_{p,f}^T$.

Now with the help of a computer and using a simple program or a computer algebra system, we can calculate the individual Hermite normal form $H_{p,f}$ for

$$(p, f) \in \{(31, 5), (127, 9), (127, 21), (139, 23), (151, 15)\}.$$

Let us take $(p, f) = (31, 5)$ and $(151, 15)$ for example. Thus we obtain the relation

$$(4.12) \quad (x_1, x_2, x_3) \begin{pmatrix} 18 & 8 & 15 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix} = 0$$

for $(p, f) = (31, 5)$ and

$$(4.13) \quad X_{151} \begin{pmatrix} 3934 & 1304 & 3470 & 3544 & 1477 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = 0$$

for $(p, f) = (151, 15)$, where $X_{151} := (x_1, x_2, \dots, x_5)$ and we omit x_{u+1}, \dots, x_g and other parts of $H_{p,f}$ since $x_{u+k} = -x_k$.

Using these computational results, we can turn to the

Proof of Theorem 1.5. We have to verify the assumption in Proposition 4.4.

- (1) If $(p, f) = (31, 5)$ the first column of the matrix in (4.12) tells us that $18x_1 = 0$ in $Cl(E)$.

Recall that $K = \mathbb{Q}(\zeta_p)$, $h_p = h(K)$ and $h_p^+ = h(\mathbb{Q}(\zeta_p + \zeta_p^{-1})) = 1$. We can write $h_p = h_p^+ h_p^-$ (see Proposition 2.7 (a)). By [21, Tables §3, pp. 412-420] we know h_{31}^- is odd. Since $h(E) \mid h(K) = h_p = h_p^-$, we know $h(E)$ is also odd. It follows that $9x_1 = 0$ and $\text{ord}(x_1) = 1, 3$ or 9 in $Cl(E)$.

We claim that $\text{ord}(x_1) = 9$. Recall $F = \mathbb{Q}(\sqrt{-p}) = \mathbb{Q}(\sqrt{-31}) \subseteq E$ and let $\mathfrak{q}_F = \mathfrak{Q}_1 \cap \mathfrak{o}_F$. By the table in [4, Section 12.1.2] we know that $\Xi_{31}(x)$ is the Hilbert class polynomial of F . Thus $h(F) = \deg(\Xi_{31}(x)) = 3$ and the same argument as in the proof of Lemma 3.11 tells us that \mathfrak{q}_F is not principal if and only if $\Xi_{31}(x) \equiv 0 \pmod{q}$ is not solvable. By the assumption in Theorem 1.5 we know this is the case and then \mathfrak{q}_F has order 3 in $Cl(F)$. If $\text{ord}(x_1) = 1$, i.e. $\mathfrak{Q}_1 = 1$ in $Cl(E)$, then taking norm gives $\mathfrak{q}_F = 1$ in $Cl(F)$, which is a contradiction. If $\text{ord}(x_1) = 3$, then $\langle x_1 \rangle \cong \mathbb{Z}/3\mathbb{Z}$ and we may assume $x_1 = 1 \pmod{3}$. The second column of the matrix reads $8x_1 + 2x_2 = 0$. Since 2 can be canceled from every equation, we have $x_2 = -4x_1$. Hence $x_2 = -x_1 = -1 \pmod{3}$ and similarly $x_3 = 1 \pmod{3}$. Thus $x_k = \pm 1 \pmod{3} \in \mathbb{Z}/3\mathbb{Z}$ for all $k = 1, 2, \dots, 6$. But we know three of all six x_k 's (i.e. \mathfrak{Q}_k 's) lie over \mathfrak{q}_F . Suppose that $\mathfrak{q}_F \mathfrak{o}_E = \mathfrak{Q}_{k_1} \mathfrak{Q}_{k_2} \mathfrak{Q}_{k_3}$. If all these three $x_{k_1}, x_{k_2}, x_{k_3}$ are the same, say $1 \pmod{3}$, then $\mathfrak{q} \mathfrak{o}_E = 1$ in $Cl(E)$. Since $Cl(F) \rightarrow Cl(E)$ is injective (Proposition 2.3), we have $\mathfrak{q}_F = 1$ in $Cl(F)$, a contradiction. Otherwise we may assume $x_{k_1} = -x_{k_2} = 1$ and then $x_{k_1} + x_{k_2} = 0$. Taking norm gives $\mathfrak{q}_F^2 = 1$, which is also false.

Thus we have $\text{ord}(x_1) = 9$ and using the matrix again we obtain

$$(x_1, x_2, \dots, x_6) = (1, -4, -2, -1, 4, 2)$$

are all in $\langle x_1 \rangle \cong \mathbb{Z}/9\mathbb{Z}$. We now apply Proposition 4.4. Let $l = 1, 3, \dots$ and solve the equation (4.3) modulo 9. A simple calculation tells us that $l_0 = 1$ is the maximal nonnegative odd number such that (4.3) is not solvable in $Cl(E)$. Hence we obtain by Proposition 4.4 the non-existence of GBFs with type $[31, 31^a q^l n']$.

- (2) The argument for $(p, f) = (151, 15)$ is similar. Using the matrix in (4.13) we know that $2 \times 7 \times 281x_1 = 0$. The same method yields the fact that $h(E)$ is also odd. Thus we find that $\text{ord}(x_1) = 7, 281$ or 1967 . In this case $F = \mathbb{Q}(\sqrt{-157})$. Knowing that $h(F) = 7$ and \mathfrak{q}_F has order 7 in $Cl(F)$ since $\Xi_{151}(x) \equiv 0 \pmod{q}$ is not solvable, the candidate order 1 and 7 can be removed by the previous method. If we have $281x_1 = 0$, taking norm gives $\mathfrak{q}_F^{281} = 1$, which contradicts to $\text{ord}(\mathfrak{q}_F) = 7$. Thus $\text{ord}(x_1) = 1967$ and we obtain $x_1, \dots, x_{10} \in \langle x_1 \rangle \cong \mathbb{Z}/1967\mathbb{Z}$ and

$$(x_1, x_2, \dots, x_5) = (1, -652, 232, 195, 715)$$

$$x_{5+k} = -x_k, \quad k = 1, 2, \dots, 5.$$

Let $l = 1, 3, \dots$ and solve the equation (4.3) modulo 1967. We find that $l_0 = 5$ is the maximal nonnegative odd number such that (4.3) is not solvable in $Cl(E)$. Again Proposition 4.4 implies the non-existence of GBFs with type $[151, 151^a q^l n']$.

- (3) For other $(p, f) \in \{(127, 9), (127, 21), (139, 23)\}$, the proofs are similar.

□

5. CORRESPONDING NON-EXISTENCE RESULTS FOR PAPSS

In this section, we give briefly two non-existence results for PAPSSs, which are similar to Theorem 1.3 and 1.5, respectively. Their proofs are also similar.

Proposition 5.1 (See [12] Theorem 1.4 (2)). If there exist PAPS with type $[p, n+1]$, then $p \mid n-1$ and $\alpha\bar{\alpha} = n$ for some $\alpha \in \mathbb{Z}[\zeta_p]$.

Theorem 5.2. Let $p \equiv 5 \pmod{8}$ be a prime and $\tilde{Q}_p = \{q \text{ is a prime} \mid \text{ord}_p(q) = (p-1)/4\}$. Then there exists a lower bound p_0 , and an infinite set $Q_p \subseteq \tilde{Q}_p$ for each p , such that if $p > p_0$,

there is no PAPSSs with type $[p, qn' + 1]$ for all integers $q \in Q_p$, n' such that $n' = 1$ or $(\frac{p'}{p}) = -1$ for all prime divisor p' of n' and $p \mid qn' - 1$.

Proof (sketch). If there exist PAPS with type $[p, qn' + 1]$, where $p \equiv 5 \pmod{8}$ be a prime, then by Proposition 5.1 we know that $p \mid qn' - 1$ and

$$\alpha\bar{\alpha} = qn' \text{ for some } \alpha \in \mathfrak{o}_K = \mathbb{Z}[\zeta_p].$$

Here $K = \mathbb{Q}(\zeta_p)$. By [12, Lemma 2.4 (1)] we obtain that

$$\alpha_2\bar{\alpha}_2 = q \text{ for some } \alpha_2 \in \mathfrak{o}_K.$$

Then the remaining argument is totally the same as the proof of Theorem 1.3. See Section 3. \square

Theorem 5.3. *Let $p \equiv 3$ be a prime, $q \neq p$ another prime and $f = \text{ord}_p(q)$. Suppose that the triple (p, f, l_0) equals to one of the following value:*

$$(31, 5, 1), (127, 9, 1), (127, 21, 3), (139, 23, 1), (151, 15, 3).$$

Define

$$\begin{aligned} \Xi_{31}(x) &= x^3 + x - 1, \\ \Xi_{127}(x) &= x^5 - x^4 - 2x^3 + x^2 + 3x - 1, \\ \Xi_{139}(x) &= x^3 - x^2 + x + 2, \\ \text{and } \Xi_{151}(x) &= x^7 - x^6 + x^5 + 3x^3 - x^2 + 3x + 1. \end{aligned}$$

Suppose further that for each $p \in \{31, 127, 139, 151\}$, the corresponding q satisfies that $\Xi_p(x) \equiv 0 \pmod{q}$ is not solvable. Then there is no PPPs with type $[p, q^l n' + 1]$ for all integers l odd, $1 \leq l \leq l_0$, n' such that $n' = 1$ or $(\frac{p'}{p}) = -1$ for all prime divisor p' of n' and $p \mid q^l n' - 1$.

Proof (sketch). The argument is totally the same as the proof of Theorem 1.5 (in Section 4), except that we use Proposition 5.1 instead of Proposition 2.11. \square

ACKNOWLEDGMENT

The author would like to thank Jianing Li for many helpful discussions and comments.

REFERENCES

- [1] CMH, available at <http://cmh.gforge.inria.fr/>.
- [2] Yeow Meng Chee, Yin Tan, and Yue Zhou, *Almost p -ary perfect sequences*, International Conference on Sequences and Their Applications, Springer, 2010, pp. 399–415.
- [3] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer, New York, 1993.
- [4] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer, 2000.
- [5] Pierre E Conner and Jürgen Hurrelbrink, *Class number parity*, Series in Pure Mathematics, vol. 8, World Scientific, 1988.
- [6] Gary Cornell and Michael Rosen, *A note on the splitting of the Hilbert class field*, Journal of Number Theory **28** (1988), no. 2, 152–158.
- [7] Andreas Enge and Damien Robert, *Computing class polynomials in genus 2*, available at http://www.normalesup.org/%7erobert/pro/publications/reports/2013-04-class_poly_g2.pdf (2013).
- [8] Gerald J. Janusz, *Algebraic number fields*, 2 ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, 1996.
- [9] Dieter Jungnickel and Alexander Pott, *Perfect and almost perfect sequences*, Discrete Applied Mathematics **95** (1999), no. 1, 331–359.

- [10] Evgeny I Krenkel, *Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphase sequences*, International Conference on Sequences and Their Applications, Springer, 2010, pp. 387–398.
- [11] Serge Lang, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, Springer, New York, 1970.
- [12] Haiying Liu and Keqin Feng, *New results on nonexistence of perfect p -ary sequences and almost p -ary sequences*, Acta Mathematica Sinica, English Series **32** (2016), no. 1, 2–10.
- [13] Chang Lv and Jianing Li, *On the non-existence of certain classes of generalized bent functions*, Information Theory, IEEE Transactions on **63** (2017), no. 1, 1–9.
- [14] Siu Lun Ma and Wei Shean Ng, *On non-existence of perfect and nearly perfect sequences*, International Journal of Information and Coding Theory **1** (2009), no. 1, 15–38.
- [15] John C Miller, *Real cyclotomic fields of prime conductor and their class numbers*, Mathematics of Computation **84** (2015), no. 295, 2459–2469.
- [16] Jürgen Neukirch, *Algebraic number theory*, Springer, 1999.
- [17] Ferruh Özbudak, Oğuz Yayla, and C Cengiz Yıldırım, *Nonexistence of certain almost p -ary perfect sequences*, International Conference on Sequences and Their Applications, Springer, 2012, pp. 13–24.
- [18] *PARI/GP*, available at <http://pari.math.u-bordeaux.fr/>.
- [19] René Schoof and Lawrence C Washington, *Visibility of ideal classes*, Journal of Number Theory **130** (2010), no. 12, 2715–2731.
- [20] Marco Streng, *Computing igusa class polynomials*, Mathematics of Computation **83** (2014), no. 285, 275–309.
- [21] Lawrence C Washington, *Introduction to cyclotomic fields*, 2 ed., Graduate Texts in Mathematics, vol. 83, Springer, New York, 1997.

STATE KEY LABORATORY OF INFORMATION SECURITY, INSTITUTE OF INFORMATION ENGINEERING, CHINESE ACADEMY OF SCIENCES, BEIJING 100093, P.R. CHINA

E-mail address: lvchang@iie.ac.cn